

IN THE SPECIFICATION

~~Please change the title to read:~~

~~—Creating and Storing One or More Digital Certificates Assigned to a Subscriber for Efficient Access Using a Chip Card—~~

~~Please replace the paragraph beginning on page 9, line 11 with the following paragraph:~~

a 1
A second certificate in certificate chain 108 is the Bank certificate 118 which has components similar to user digital certificate 110. Certificate 118 contains a Bank public key 120 and attributes 115, attributes that are relevant to another entity, such as a trusted root, having a certificate in certificate chain 108. An encrypted data segment 122 in Bank certificate 118 ~~has~~ is attributes 115 ~~that are~~, this time encrypted or signed using a public key belonging to a trusted root, such as a banking associations (e.g., Visa) or a government agency. This root is an entity that both the merchant and Bank trust in, simply, telling the truth about the identity of certain parties. The merchant may not necessarily trust the Bank in that it may not have complete confidence in the Bank's identity. However, the merchant does trust the root, and if the root is willing to verify the Bank's identity, the merchant will trust the Bank and ultimately the card holder.

~~Please replace the paragraph beginning on page 5, line 10 with the following paragraph:~~

a 2
In another aspect of the invention, a method of authenticating a user presenting a chip card to an entity, such as a merchant or service provider, is described. A certificate library address is read from the chip card. At the certificate library, the entity provides additional parameters to identify a particular certificate needed by the entity to authenticate the user. Once the correct certificate is located it is returned to the reliant party so that they may authorize the card holder's attributes. The methods of traversing the certificate chain are known in the field. For example, one such certificate chain is a Public Key Infrastructure (PKI). Another cryptographic infrastructure can be based on a DES DED shared key system.

~~Please replace the paragraph beginning on page 13, line 14 with the following paragraph:~~

a 3
FIG. 2 is a diagram showing a single chip card having access to multiple PKIs. Chip card 102 stores a certificate library address 106 which can access a certificate library directory 202. At certificate library address 106 are stored multiple PKIs all having the same user public key, shown as Public Key A. As described above, Public Key A and corresponding private key 104 were verified initially to belong to the correct user by the registration authority. This is the initial overhead or due diligence performed by the registration authority. Any number n of PKIs can be added to certificate library directory 202. The trusted root in each PKI can be the same as or different from any other trusted root. The trusted root is established via a relationship between the entity creating the PKI and the root.

A4
Please replace the paragraph beginning on page 16, line 7 with the following paragraph:

The certificate store configuration of the present invention offers the ability to support numerous PKIs using a single private key and certificate library address which combined make up approximately two kilobytes of memory on the chip card. As described above, certificate store application 318 on card 316 represents a private key and an address that links it to a digital certificate containing a public key in certificate library directory 322. If reliant party 308 wants to authenticate the card holder, it can access card application 318, request an appropriate certificate from certificate library directory 202 by appending LDAP query parameters to the address on the card, and traverse the certificate chain using the process described above. If the certificate exists, it is accessed so the reliant party or primary party can validate the card's private key. This process is described in greater detail below

A5
Please replace the paragraph beginning on page 15, line 21 with the following paragraph:

Certificate library directory 202 is an LDAP server able to store the certificate so that a reliant or primary party can authenticate a relationship between the party and a user exists. For example, a merchant can read an address on the card, access a memory location in the certificate library, and determine whether the card holder has a digital certificate issued by that merchant or recognizable to that merchant. In the described embodiment, certificate library directory 202 322 relies on LDAP to communicate with reliant party 308 and certificate authority 304. Chip card 316 can store credit, debit and other stored applications. Chip card 316 can also have "value added" applications to provide reliant party 308 and the user with other applications in addition to user authentication. Since chip cards are resource-constrained devices, it is desirable to minimize data on the chip card.